Exhibit 30

Excerpts of PWC-SEC-00041801

pwc

Evaluating Internal Control Deficiencies Consultation Memo

Note: This optional memo has been developed to assist engagement teams in documenting their evaluation of internal control deficiencies and is suggested to be used for formal consultations with Auditing Services, Methods & Tools ("ASM&T"). This template is aligned with the principles of likelihood and magnitude included in PCAOB Auditing Standard No. 2201, *An Audit of Internal Control Over Financial Reporting That Is Integrated with An Audit of Financial Statements* ("AS 2201") and will facilitate an effective and efficient consultation on the evaluation of control deficiencies considered to be "close call" (based on the guidance in PwC Public Audit Guide 8301.2) or material weakness(es) to be communicated in an integrated audit and PCAOB non-integrated audits[1]. The memo is not a replacement for reading the applicable literature, PwC Public Audit Guide sections (principally PwC Public Audit Guide 8300), and the internal Practice Aid for Evaluating Control Deficiencies ("Practice Aid").

For consultations with ASM&T, the following documents are subject to the consultation and should be attached within Consult:

- Client deficiency evaluation memo
- PwC deficiency evaluation wrap memo (herein)
- Disclosure Controls and Procedures, Changes in Internal Control Over Financial Reporting, Management's Report on Internal Control Over Financial Reporting, and Remediation Plan (applies only if there is a material weakness conclusion). These disclosures typically reside within Item 4 of Form 10-Q (if the initial disclosure of the material weakness is made during an interim period) or Item 9A of Form 10-K (if the initial disclosure of the material weakness is made in the annual financial statements); however, they may reside elsewhere within the company's filing with the SEC
- Audit report (applies only if there is a material weakness conclusion and we have been engaged to audit internal control over financial reporting)

Additionally, to assist in understanding and assessing the conclusions reached herein, the ASM&T consultant may ask to be provided with relevant SAB 99 memos (if the deficiency(ies) are the result of actual misstatements) and/or to review other related deficiencies included on the Summary of Aggregated Deficiencies.

The memo is to be used by engagement teams to document their evaluation and conclusions when evaluating a control deficiency(ies) individually and in the aggregate and possible material weakness(es), in accordance with the consultation requirements in PwC Public Audit Guide 8301.2. This memo does not replace management's evaluation and documentation of their considerations and conclusions regarding the evaluation of the deficiency(ies). In fact, this memo should serve as our wrap memo to document our audit evidence related to management's assertions in their evaluation.

[1] The concepts included in this memo may also be useful in the evaluation of control deficiencies identified in private company audits performed under AICPA standards.

pwc

- *Based on management's analysis of the magnitude of the potential misstatement and in applying due care and professional skepticism, consider evidence of whether the magnitude is limited to this error, the potential magnitude identified, or other factors. We need evidence to support the potential magnitude and how this links to the root cause.*

Response:

Yes, Refer to the risk assessment above.

Box 4: Is the deficiency (or combination of deficiencies) important enough to merit the attention by those responsible for oversight of the company's financial reporting? (AS 2201.A11) If yes, go to Box 6. If no, then the deficiency is a "control deficiency" (AS 2201.A3) and go to Box 7.

- *Document whether based on our professional judgment and depending upon the facts and circumstances of the deficiency (or combination of deficiencies) specific to the company, whether it is important enough to merit the attention of those responsible for oversight of the company's financial reporting (Yes or No).*

Response:

Yes, the Cyber Incident and the related evaluation of ITGCs has been discussed at the Board level (daily calls from mid-December to early January). The ITGC considerations were also discussed at the Audit Committee meeting on January 10, 2021 and communicated in writing on Tuesday, February 23, 2020.

A significant deficiency was identified as a result of the aggregation of the following IT related deficiencies:

- Lack of adequate preventative and/or detective authentication controls over domain administrator accounts to restrict financial reporting infrastructure access to only approved and authorized users
- Lack of adequate preventative and/or detective controls over generic accounts to restrict financial reporting systems access to only approved and authorized users
- Lack of adequate preventative and/or detective authentication controls over user accounts to restrict access to financial reporting systems to only approved and authorized users.

Box 5: Do compensating controls exist and operate effectively at a level of precision sufficient to prevent or detect a misstatement that could be material to either interim or annual financial statements? (AS 2201.68) If yes, go to Box 4. If no, then the deficiency is a "material weakness" (AS 2201.A7).

- *We may consider whether one or more compensating controls mitigate the severity of a deficiency in a control activity provided that we have tested the compensating controls and concluded they were designed and operated effectively.*
- *Document a description of any compensating controls that we intend to rely on to reduce the severity of the deficiency. If there was an actual misstatement, consider whether the compensating control identified the misstatement in question or whether or not it should have. It is critical that when we are evaluating the compensating controls, we need to obtain evidence that the controls are not only designed effectively to compensate, but also are operating effectively.*

pwc

Change Management
• Deficiencies exist related to the approval, testing and monitoring for changes to RMM Infrastructure (note that these deficiencies are not at the application layer). These change management deficiencies did not aggregate with the deficiencies identified above related to the cyber incident due to the following factors: RMM infrastructure is not on Windows, this does not impact the application layer, RMM follows a unique change management process and does not relate to generic accounts or authentication.

Response – By business unit:

The nature of the deficiency relates to the risk of unauthorized access as a result of a cybersecurity incident. As a result, the engagement performed the analysis above in the sections Business Overview and Box 2 to determine the specific FSLIs, disclosures, business processes, and business units most likely to be impacted. Refer above.

Conclusion

Briefly describe management's conclusion and the engagement team's conclusion and the basis for the conclusion. Also, describe the impact of the deficiency, if any, to the financial statements (e.g., resulted in audit adjustments to [list account impacted], resulted in a restatement or revision of the consolidated financial statements for the periods [list periods], etc.) Also, address the possible implications and impact of the conclusion on our report on internal control over financial reporting for the prior year, if applicable (AS 2201.98).

Response:

Based on the identification of compensating controls, coupled with the results of management's lookback procedures, concluded that this is limited to a significant deficiency.

Partner Concurrence

Document the engagement team partners, including QRP, and ASM&T partners who were involved in the consultation and note their concurrence with the preliminary views expressed. In order to ensure compliance with the relevant auditing standards, concurrence should be obtained prior to the financial statement issuance date.

Response:

The engagement team was supplemented by others from our Cyber practice (John Boles) and forensics (Kim Wiatrak) during the course of the investigation and identification of facts.

The following partners were involved in this ICFR consultation and concurred with the conclusion:

pwc

entries that were not created or posted by these compromised users. Based on our additional testing, we were able to validate that there were no instances of a compromised user creating a journal entry.

2. Forecast to Actual Quarterly Lookback: The ET compared eight quarters (Q1 2019 to Q4 2020) of management's public forecasted results (quarterly guidance) to actual results. On a base of $215 million (Q1'19) to $265 million (Q4'20), the Company's actual results were within 1-2% of forecasted results. This outcome is reasonable considering the recurring nature of the majority of the revenue (subscriptions).

3. Revenue: As part of our CORE IT revenue testing, PwC targeted transactions greater than $250K as part of its original audit procedures. Due to the planned MSP Spin, we performed additional transactional level testing at a lower materiality which resulted in 69 additional samples (that would not have been otherwise required for the consolidated SWI audit). There were no exceptions noted within the Core IT or MSP revenue results. We further noted that each transaction tested was traced back to cash/bank statements, without exception, and there were no customers noted requesting refunds. Additionally, at the consolidated level (Core & MSP) the ET obtained and assessed the credit memo listing. We noted the credit memos issued after period end (January 2021) were less than $1M.

4. Accounts Receivables & Collections: The engagement team assessed uncollected AR as of December 21, 2020 over 60 days which amounted to only $1.7M and $700K for Core IT and MSP, respectively. Further, we obtained the January AR Aging and noted there was no significant change or increase in aging.

5. Accounts Payable: The engagement team target tested wires over $5M amount to validate the accuracy, business purpose, and appropriate approver. Further, we reviewed the AP Aging detail for any vendors aged over 60 days.

6. Legal Letter Confirmations: The ET sent additional legal representation letters to the following firms: A, B, C.

Audit Committee Communication

Whether we are performing an integrated audit or an audit of the financial statements only, we must communicate in writing to management and the Audit Committee all material weaknesses and significant deficiencies in internal control over financial reporting identified during the audit. For public company financial statement audits and integrated audits this communication is required before the issuance of our audit report (AS 1305, AS 2201). For public company audits, we are also required to make this communication before the filing of the company's 10-Q as it relates to interim reviews (AS 4105).

The memo should confirm this written communication occurred in accordance with PwC Public Audit Guide 1502.1 and applicable auditing standards; however, it does not need to be duplicative of documentation that already exists in your audit file.

Response:

pwc

We attended the Audit Committee meeting on February 10, 2021 and February 23, 2021 where the Cyber Incident was discussed and the significant deficiency was communicated in writing.

- Lack of adequate preventative and/or detective authentication controls over domain administrator accounts to restrict access to financial reporting infrastructures to only approved and authorized users
- Lack of adequate preventative and/or detective controls over generic accounts to restrict access to financial reporting systems to only approved and authorized users
- Lack of adequate preventative and/or detective authentication controls over user accounts to restrict access to financial reporting systems to only approved and authorized users

Plan to Publicly Disclose

Based on the nature of the cybersecurity incident, does Management plan to disclose the incident in a SEC filing? If yes, please include the disclosure and who from SEC services has reviewed the disclosure?

Response:

Yes, the company discussed the cyber incident in two 8-K releases providing information related to the compromised products, the nature of the incident, investigation to date, and steps taken to address the vulnerabilities in the software used by customers.

a. December 17, 2021 - 8k (link)
b. January 11, 2021 - 8k (link)

The December 14 8-k was reviewed by Kyle Moffatt (SEC Services) and Randol Justice (our Regional QMP) prior to the 8-K filing.

The Company has also included disclosure of the Incident in several places within the Form 10-K. The Form 10-K has been reviewed by Kyle Moffatt, as well. Refer to Appendix below for draft Form 10-K disclosures.

The Company also disclosed updates via their website and blog posts since the incident.

The significant deficiency will not be communicated externally.

pwc

SWI Privilege